**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF MICHIGAN**

| | |
|---|---|
| **DANNY ROLL**, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>**FLAGSTAR BANCORP, INC.** and **FLAGSTAR BANK, FSB,**<br><br>Defendants. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Danny L. Roll brings this Class Action Complaint and Demand for Jury Trial ("Complaint") against Defendants FlagStar Bancorp, Inc. and Flagstar Bank, FSB ("Defendants" or "Flagstar") and alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

## NATURE OF THE ACTION

1. FlagStar, a Michigan-based federal savings bank with 150 branches nationwide, has woefully failed to take even the most elementary precautions to protect private and confidential personal information of more than 1.5 million U.S. customers.

2. Indeed, on December 3, 2021 and December 4, 2021, hackers accessed Flagstar's networks and servers and exfiltrated highly-sensitive personal information of more than 1.5 million U.S. customers (the "Data Breach"). The Data Breach included social security numbers, account/loan numbers, names, addresses, phone numbers, dates of birth, and financial institution names.

3. On June 2, 2022, nearly six (6) months after the unauthorized access, Flagstar concluded an investigation into the Data Breach.

4. On June 16, 2022, FlagStar notified its customers of the Data Breach and informed them that their personal information was affected.

5. The Data Breach was the result of Flagstar's failure to implement reasonable security procedures and practices. Flagstar failed to disclosure material facts surrounding its deficient data security protocols. Such a failure to protect its customers' information violates Flagstar's obligations as established by law.

6. Additionally, Plaintiff's and the Class's Private Information is now in the hands of unknown third parties.

**7.** As a result of Flagstar's failure to implement and follow basic security procedures as described herein, Plaintiff and class members did not receive the benefit of their bargain with Flagstar and now face significant risk of identity theft, financial fraud, and other identity-related fraud now and in the future.

**8.** As such, Plaintiff, on behalf of himself and all other class members,

asserts claims for negligence, breach of implied contract, and breach of express contract.

## PARTIES

9. Plaintiff Danny Roll is a natural person and citizen of Ishpeming, Marquette County, Michigan.

10. Defendant Flagstar Bancorp, Inc. is a corporation formed in Michigan with its principal place of business located at 5151 Corporate Drive, Troy, Michigan 48098. Defendant conducts business throughout this District and the United States.

11. Defendant Flagstar Bank, FSB is a Michigan-based, federally chartered stock savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098. Defendant conducts business throughout this District and the United States.

## JURISDICTION AND VENUE

**12.** This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class, which consists of over 100 persons, is a citizen of a state different from Defendants, (b) the amount in controversy exceeds $5,000,000 exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

**13.** This Court has personal jurisdiction over Defendants because they are

domiciled in this District, their principal places of business are located in this District, they are headquartered and regularly conducts business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from this District.

**14.** Venue is proper pursuant to 28 U.S.C. § 1391(b) because the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from this District. Venue is additionally proper because Plaintiff and Defendants reside in this District.

## COMMON FACTUAL ALLEGATIONS

**15.** Flagstar is a federally charted savings bank headquartered in Troy, Michigan. Flagstar has more than 150 branches across the country, including in Michigan, Indiana, California, Wisconsin, and Ohio.

**16.** Flagstar is the sixth largest bank mortgage originator and the third largest savings bank in the United States with more than $31 billion in assets.

**17.** In the course of business, Flagstar collects highly sensitive personal information, such as social security numbers, credit scores, account/loan numbers, names, addresses, phone numbers, and dates of birth. Flagstar stores this personal information on its networks and servers.

**18.** On its website, Flagstar posts a privacy policy dated February 2018, which describes when and how it obtains personal information from customers.

Flagstar states as follows:

> We collect your personal information, for example, when you:
>
> • Open an account or deposit money
> • Pay your bills or apply for a loan
> • Use your debit card
>
> We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.[1]

19. On the same privacy disclosure, Flagstar claims to protect its customers' information as follows: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[2]

20. On its webpage entitled "Preventing Fraud," Flagstar also claims to "have firewalls and prevention systems that stop unauthorized access to our network and computers, plus secure network protocols that ensure secure connections between our offices, partners, and customers."[3]

21. By obtaining, collecting, and storing the personal information of Plaintiff and class members, Defendant assumed legal and equitable duties and

---

[1] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last visited July 1, 2022).

[2] *Id.*

[3] https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last visited July 1, 2022).

knew or should have known it was responsible for protecting the personal information from unauthorized disclosure.

***The Data Breach***

22. Between December 3, 2021, and December 4, 2021, hackers gained access to Flagstar's network and servers. The hackers were able to access and exfiltrate highly sensitive customer information, including names, addresses, social security numbers for more than 1.5 million customers.

23. On June 16, 2022, more than six months after it occurred, Flagstar finally disclosed the existence of the Data Breach to its customers. Flagstar claimed that it notified federal authorities and "engaged external cybersecurity professionals" to investigate the breach.[4]

24. Nevertheless, Flagstar has not disclosed the extent of the investigation into the breach. Rather, it simply states that it has concluded the investigation and is in the process of notifying individuals that were impacted by the breach by mail.[5]

25. Flagstar also makes the bold claim that "we have no evidence that any of your information has been misused."[6] However, Flagstar provides customers with no information as to how it has arrived at this conclusion. Indeed, the statement cannot be squared with Flagstar's concession that the personal

---

[4] https://www.flagstar.com/customer-support/customer-data-information-center.html

[5] *Id.*

[6] *Id.*

information was "acquired" from its network. In other words, Flagstar tacitly admits that its affected customers, such as Plaintiff, have been harmed. Indeed, their sensitive, personal information is in the possession of the hackers.

26. Flagstar similarly provides no explanation for why it failed to discover or disclose the Data Breach for more than six months. By delaying the disclosure, Flagstar robbed customers of the ability to take meaningful, proactive, and targeted mitigation measures to protect themselves from identity theft.

27. This is also not Flagstar's first lapse of security with respect to its customers' private personal information. Indeed, in January 2021, a hacking group breached and exfiltrated the servers of Flagstar's vender, Accellion, and obtained personal information, including social security numbers, addresses, tax records, and phone numbers, for millions of its customers.

28. Added to this, the financial services industry is one of the most targeted industries for cyberattacks given the sensitive nature of the information that companies collect and maintain regarding their customers.[7]

29. Put simply, at all times relevant to this Complaint, Flagstar knew, or should have known, that its customers' and former customers' personal information was targeted by malicious actors. Nevertheless, Flagstar failed to take

---

7 https://www.mycouriertribune.com/news/national_news/data-breaches-are-more-costly-for-these-10-industries/collection_442030e1-b639-5e79-86d0-e848222174b6.html#11

steps to implement and maintain reasonable data privacy and security measures to protect Plaintiff's and the Class's personal information from cyber-attacks.

**FACTS SPECIFIC TO PLAINTIFF ROLL**

30. Plaintiff Roll is a current customer of Flagstar.

31. When Plaintiff established an account with Flagstar, he provided his personal information to Flagstar. Plaintiff did so with the understanding and expectation that Flagstar would use reasonable safeguards and protocols, as promised by its Privacy Policy and related documents, to protect his information.

32. Had Plaintiff known of Flagstar's substandard security procedures and methods of protecting and storing his private information, he would not have opened an account with Flagstar.

33. On or around June 16, 2022, Plaintiff received a letter from Flagstar notifying him that he was a victim of the Data Breach. The letter informed him that "one or more of the impacted files contained [his] social security number, account/loan number, name, address, phone number, date of birth, and financial institution name."

34. The letter also recommended that Plaintiff place "a fraud alert and/or security freeze on your credit files." Plaintiff did activate the fraud alerts with the credit bureaus, and he has expended time to monitor his financial accounts.

35. As a result of Flagstar's carelessness, Plaintiff and the Class must now

live with the knowledge that their personal information is forever in the possession of the people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

36. As such, Plaintiff and the class members have sufficient injury and damages, including a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services that were received without adequate data security.

## CLASS ALLEGATIONS

37. **Class Definition**: Plaintiff Roll brings this action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2), and 23(b)(3) on behalf of herself and a Class of similarly situated individuals defined as follows:

> All individuals residing in the United States whose personal information was compromised in the Data Breach.

38. The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2)

Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons. Plaintiff anticipates the need to potentially amend the class definition following necessary and appropriate discovery.

39. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but on information and belief, the Class is comprised of millions of individuals throughout the country, making joinder of each individual member impracticable. The members of the Class will be easily identified through Defendants' records as Defendants will have data reflecting the identities of the members' whose personal information has been compromised.

40. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class for which a class action would provide common answers. Such common questions of law and fact include, but are not limited to:

a. Whether Defendants owed Plaintiff and Class Members a duty to implement and maintain reasonable security procedures and practices

to protect their personal information;

b. Whether Defendants breached their privacy agreement with Plaintiff and Class Members to keep their personal information confidential;

c. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' personal information;

d. Whether Defendants violated their duty to implement reasonable security systems to protect Plaintiff's and Class Members' personal information;

e. Whether Defendants' breach of their duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class Members;

f. Whether Defendants provided timely notice of the Data Breach to Plaintiff and Class Members; and

g. Whether Class Members are entitled to compensatory damages and punitive damages as a result of the Data Breach.

41. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained substantially the same injury and similar damages as a result of Defendants' uniform wrongful conduct in failing to safeguard Plaintiff and the other class members' personal information.

42. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions. Plaintiff is a member of the Class and has no interest antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff.

43. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' practices challenged herein apply to and affect the Class members uniformly, and Plaintiff's challenge of those practices hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

**44. Predominance:** The common issues set forth above go to the heart of the litigation and predominate over any supposed individualized questions. That is, Flagstar didn't take special precautions with respect to certain member data that it didn't take with respect to others. As the same (faulty) standards were applied to everyone, the common questions predominate.

45. **Superiority & Manageability**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy given that joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants'

actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

## FIRST CAUSE OF ACTION
**Negligence**
***(On Behalf of Plaintiff and the Nationwide Class)***

46. Plaintiff repeats and realleges every allegation set forth in the preceding Paragraphs.

47. Defendants required Plaintiff and Class Members to provide their personal information as a condition of receiving financial services. Defendants collected and stored the data for various purposes, including providing financial services as well as for commercial gain.

48. Defendants owed Plaintiff and Class Members a duty to exercise reasonable care in protecting their personal information from unauthorized disclosure or access.

49. Defendants owed a duty of care to Plaintiff and Class Members to provide adequate data security and to ensure that Defendants' systems and networks adequately protected the personal information.

50. Given the nature of Defendants' business, Defendants should have known that Plaintiff's and the Class Members' personal information was sensitive. And their duty to use reasonable care in protecting personal information arises as a result of the parties' relationship, as well as common law and federal law, and Defendants' own policies and promises regarding privacy and data security.

51. Indeed, Defendants knew, or should have known, of the risks inherent in collecting and storing personal information in a centralized location, Defendants' vulnerability to network attacks, and the importance of adequate security.

52. Defendants breached their duty to Plaintiff and Class Members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal information of Plaintiff and Class Members;

b. Failing to comply with industry standard data security measures for the financial industry leading up to the Data Breach;

c. Failing to comply with its own Privacy Policy;

d. Failing to adequately monitor, evaluate, and ensure the security of Defendants' network and systems;

e. Failing to recognize in a timely manner that personal information had been compromised; and

f. Failing to timely and adequately disclose the Data Breach.

53. Plaintiff's and Class Members' personal information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

54. Defendants' failure to take proper security measures to protect the sensitive personal information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of personal information by unauthorized third parties. Given that the financial services industry is a prime target for hackers, Plaintiff and Class Members are part of a foreseeable group that was at high risk of having their personal information misused or disclosed if not adequately protected by Defendants.

55. It was also foreseeable that Defendants' failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Class Members.

56. As a direct and proximate result of Defendants' conduct described

above, Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services that were received without adequate data security.

## SECOND CAUSE OF ACTION
### Breach of Implied Contract
### (On Behalf of Plaintiff and the Class)

57. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

58. Defendants required Plaintiff and Class Members to provide their personal information as a condition of receiving financial services. Defendants collected and stored the data for various purposes, including providing financial services as well as for commercial gain.

59. By requiring and accepting the information, Defendants agreed to safeguard and protect the personal information of Plaintiff and Class Members. Implicit in the parties' relationship was the obligation that Defendants would use

the personal information for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

60. Additionally, Defendants implicitly promised to retain this personal information only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the personal information of Plaintiff and Class Members from unauthorized disclosure or access.

61. Plaintiff and Class Members entered into implied contracts with the reasonable expectation that Defendants' data security practices and policies were reasonable and consistent with industry standards.

62. Plaintiff and Class Members would not have provided and entrusted their personal information to Defendants in the absence of the implied contract. The safeguarding of Plaintiff's and Class Members' personal information was critical to realizing the intent of the parties.

63. The nature of Defendants' implied promise itself, was to protect Plaintiff's and Class Members' personal information to prevent harm and prevent present and continuing increased risk.

64. Defendants breached the implied contract with Plaintiff and Class Members by failing to reasonably safeguard and protect their personal information,

which was compromised as a result of the Data Breach.

65. As a direct and proximate result of Defendants' breaches, Plaintiff and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class Members alternatively seek an award of nominal damages.

## THIRD CAUSE OF ACTION
**Breach of Express Contract**
**(On Behalf of Plaintiff and the Class)**

66. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

67. The parties entered into written agreements regarding the services that Flagstar was to provide to Plaintiff and Class Members.

68. Plaintiff and Class Members paid Flagstar monies and provided Flagstar with their personal information as consideration for the agreements.

69. Flagstar's privacy policy is evidence that data security was a material term of these contracts.

70. Plaintiff and Class Members complied with the express contract when they paid Flagstar and provided their personal information to Flagstar.

71. Flagstar breached its obligations under the contracts with Plaintiff and the Class Members by failing to implement and maintain reasonable security measures to protect and secure their personal information.

72. Flagstar's breach of the express contracts caused the Data Breach.

73. Plaintiff and all other Class Members were damaged by Flagstar's breach of express contracts because: they paid—directly or indirectly—for data security protection they did not receive; they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; their personal information was improperly disclosed to unauthorized individuals; the confidentiality of their personal information has been breached; they were deprived of the value of their personal information, for which there is a well-established national and international market; and lost time and money incurred to mitigate and remediate the effects of the Data Breach.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff Danny Roll, individually and on behalf of the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, and appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

B. Declaring that Flagstar's actions, as described above, constitute (i) Negligence, (ii) Breach of Implied Contract, and (iii) Breach of Express Contract;

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Flagstar from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Flagstar to protect all data collected through the course of its business in accordance with industry standards;

D. Awarding damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre and post-judgment interest to the maximum extent allowable by law; and

G. Awarding such other and further legal or equitable relief as equity and justice may require.

**JURY DEMAND**

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

**DANNY ROLL**, individually and on behalf of all others similarly situated,

Dated: July 1, 2022

By: /s/ Bradley J Friedman
One of Plaintiff's Attorneys

Bradley J. Friedman
bfriedmanesq@gmail.com
Law Offices of Bradley J. Friedman
30300 Northwestern Hwy, Suite 101
Farmington Hills, Michigan 48334
Tel: 248-932-0100
Fax: 248-932-3512

Patrick H. Peluso
ppeluso@woodrowpeluso.com
Steven L. Woodrow
swoodrow@woodrowpeluso.com
Taylor T. Smith
tsmith@woodrowpeluso.com
Woodrow & Peluso, LLC
3900 East Mexico Ave., Suite 300
Denver, Colorado 80210
Telephone: (720) 213-0675
Facsimile: (303) 927-0809

*Counsel for Plaintiff and the Alleged Classes*